provinciehuis Westerbrink 1, Assen
postadres Postbus 122, 9400 AC Assen

www.drenthe.nl
0592 - 36 55 55

provincie Drenthe

Aan:
de voorzitter en leden van
Provinciale Staten van Drenthe

Assen, 23 maart 2021
Ons kenmerk 12/5.8/2021000535
Behandeld door team Bestuur en Concernzaken (0592) 36 55 55
Onderwerp: Security situatie bij BIJ12
Status: Ter informatie

Geachte voorzitter/leden,

Hierbij informeren wij u over de security-situatie bij BIJ12.

Eind januari 2021 hebben wij u met een Statenbrief geïnformeerd dat op 25 januari 2021 een aantal ICT-systemen van IPO/BIJ12 tijdelijk 'offline' is gezet. Dit was een noodzakelijke voorzorgsmaatregel omdat er kwetsbaarheden waren geconstateerd in de beveiliging van deze systemen. Dit betekende dat bepaalde applicaties tijdelijk van buitenaf onbereikbaar waren gemaakt. Deze systemen zijn alleen via een veilig kanaal bruikbaar geweest voor overheidsinstanties en ketenpartners die er gebruik van moeten maken.

Wij informeren u over de voortgang in dit dossier. Van de eerder geconstateerde kwetsbaarheden is inmiddels het grootste deel opgelost. We verwachten dat relevante applicaties stap voor stap weer zullen worden opengesteld.
Het onderzoek naar mogelijke inbreuk op systemen in het verleden is afgerond: er zijn geen sporen van inbreuk gevonden op de onderzochte systemen. De voorlopige datalek-melding aan de Autoriteit Persoonsgegevens is daarom ingetrokken.

Toelichting

IPO/BIJ12 werkt als uitvoeringsorganisatie in opdracht van de twaalf provincies. Een onderdeel van de taken van BIJ12 is dat een aantal gemeenschappelijke applicaties en informatiesystemen bij BIJ12 zijn ondergebracht. Dit betreft onder andere databanken en registers voor natuurbeheer, monitoring, subsidieverlening, schade-uitkeringen.

Stand van zaken

De IT-omgeving van BIJ12 is veiliggesteld. Overheidsorganisaties en ketenpartners hebben via een speciale constructie toegang gekregen tot de systemen van BIJ12, zodat de applicaties op een veilige wijze informatie kunnen blijven leveren, die van belang is voor de provincies en de ketenpartners. Deze methode zorgt ervoor dat de reguliere werkprocessen in een beveiligde omgeving kunnen doorgaan. De desbetreffende organisaties ondervinden geen hinder in het uitvoeren van hun werkzaamheden.

Van de eerder geconstateerde kwetsbaarheden is inmiddels het grootste deel opgelost. Enkele publieke applicaties kunnen, naar het zich nu laat aanzien, op korte termijn weer openbaar toegankelijk worden gesteld, waaronder de publieke gedeeltes van Risicokaart, LZR en SNL 2.0. Wij verwachten dat als eerste de Risicokaart komende week zal worden opengesteld.

Het externe onafhankelijke onderzoek naar inbreuk op de systemen bij BIJ12 is afgerond. Er zijn geen sporen van inbreuk gevonden op de onderzochte systemen. De managementsamenvatting van het desbetreffende rapport is opgenomen in de bijlage.

In de vorige Statenbrief is aangegeven dat BIJ12 op 13 januari 2021 een melding had gedaan bij de Autoriteit Persoonsgegevens. Normaliter wordt een melding alleen gedaan als van een inbreuk op persoonsgegevens is gebleken. Dat was niet het geval, maar BIJ12 had er in overleg met de provinciale functionarissen gegevensbescherming voor gekozen om de Autoriteit Persoonsgegevens op de hoogte te brengen van de kwetsbaarheden en de maatregelen die BIJ12 daarop heeft genomen. Nu het onderzoek naar eventuele inbreuken is afgerond en daarbij geen inbreuk is geconstateerd, is de pro-forma-melding ingetrokken.

Vervolgprocedure/voortgang

De komende maanden wordt het repareren van de kwetsbaarheden verder afgerond. In overleg met de provinciale contactpersonen wordt daarbij op basis van gebruik en kostenoverwegingen gekozen voor herstel van bestaande applicaties of voor herbouw, uitfasering dan wel het huidige gebruik via veilige toegang continueren.

Wij zullen u op de hoogte houden van de vorderingen. In de Voorjaarsnota van IPO/BIJ12 zal door het IPO-bestuur inzicht gegeven worden in de kosten van de noodzakelijke herstelwerkzaamheden en maatregelen om een herhaling te voorkomen.

Hoogachtend,

Gedeputeerde Staten van Drenthe,

, voorzitter , secretaris

Bijlage Managementsamenvatting onderzoek mogelijke inbreuk in systemen van BIJ12

MANAGEMENTSAMENVATTING
EXTERN ONAFHANKELIJK ONDERZOEK NAAR MOGELIJKE INBREUK IN SYSTEMEN VAN BIJ12.
Uitgevoerd door Sogeti (onderdeel van CAP Gemini)
16 maart 2021

1. Managementsamenvatting

BIJ12 heeft Sogeti gevraagd een securityonderzoek uit te voeren op de omgeving van BIJ12 beheerd door Atos. Het onderzoek is gestart op 14-01-2021 en is uitgevoerd door ethical hackers / PEN testers van Sogeti.

Aanleiding voor het uitvoeren van dit onderzoek is de wens om te signaleren of er hacks hebben plaatsgevonden op de applicaties en onderliggende systemen. Dit onderzoek is geen forensisch onderzoek en is verricht vanuit het perspectief van een (ethical) hacker. Er is onderzocht of er verdachte zaken zoals een backdoor, script of onverklaarbare open poorten aanwezig waren op de systemen. De onderzoeker heeft het onderzoek uitgevoerd met de hoogste rechten en heeft daarbij ook de productiesystemen onderzocht. Ook heeft de onderzoeker verschillende penetratie testen uitgevoerd op de applicaties en systemen om inzichtelijk te krijgen welke kwetsbaarheden mogelijk misbruikt kunnen worden om toegang tot de systemen te krijgen.

Samenvatting

Na afronding van het onderzoek is de securityspecialist tot de volgende conclusies gekomen.

Het onderzoek laat zien dat er geen sporen van misbruik gevonden zijn op de onderzochte systemen.

De beschikbare logs van de omgeving van BIJ12 beheerd door Atos waren erg beperkt. Op basis van de beschikbare logs is gezocht op verdachte situaties, deze zijn niet gevonden. Het is aan te raden om meer logging toe te voegen op de productie omgeving.

De verschillende systemen en applicaties zijn onderzocht op de aanwezigheid van backdoors, deze zijn niet gevonden.

De onderzoeker heeft onderzoek gedaan naar de Advanced Web Statistics. Op basis van de gemaakte HTTP(S) requests en specifieke downloads van bestanden is er geen bewijs van misbruik gevonden.

De onderzoeker heeft blackbox penetratie testen uitgevoerd aan de “buitenkant” van de applicaties, er zijn geen kritieke vulnerabilities gevonden die tot misbruik van onderliggende systemen konden leiden.

Een onderzoek achteraf kan nooit uitsluiten dat ergens inbreuk zou zijn gepleegd door een hacker die alle sporen daarvan volledig zou hebben gewist, maar bovenstaande bevindingen maken het zeer onwaarschijnlijk dat er op deze systemen inbreuk is gepleegd.

Het is aan te raden om in de toekomst met regelmaat vulnerability assessments en penetration testen te laten doen. Ook is het aan te raden om het patch management op te zetten.

De onderzochte applicaties zijn wisselend in kwaliteit, het is aan te raden om te onderzoeken welke applicaties opnieuw gebouwd of aangepast moeten worden. Dit onderzoek is inmiddels gestart bij BIJ12.

Lopende het onderzoek is er samen met de BIJ12 architect, applicatie eigenaren en beheerders een helder en compleet overzicht opgesteld van de BIJ12 applicaties en systemen beheerd door Atos (en buiten Atos, maar deze zijn buiten scope van dit onderzoek). Op grond van de prioriteitsstelling uit deze lijst heeft het onderzoek plaatsgevonden.